Une meilleure protection des données personnelles grâce au RGPD

À l'approche de la date d'entrée en vigueur du Règlement général européen sur la protection des données, des milliers d'entreprises vont bientôt devoir se conformer aux lois régissant la gestion des données personnelles. Dans ce contexte, l'application du RGPD soulève fréquemment les questions suivantes :

- Qu'est-ce que le RGPD et qu'implique-t-il pour les entreprises et les citoyens ?
- Comment est-ce que le RGPD protège les données personnelles ?

Dahua donne ici une brève introduction au RGPD.

Contexte de l'élaboration du RGPD

L'Union européenne a introduit, en 1995, la Directive sur la protection des données (dénommée « Directive » ci-après) fixant un cadre légal pour la protection des données dans ses états membres. Le champ du traitement des données personnelles collectées se limitait alors aux noms d'utilisateurs, aux adresses comme à des informations financières relativement basiques. Vingt ans plus tard, les progrès technologiques ont cependant ouvert une nouvelle ère des réseaux d'information, dont le big data et le cloud computing. Alors que les citoyens profitent des avantages des services en ligne, ils sont aujourd'hui d'autant plus concernés par la protection des données qu'ils génèrent ou fournissent. En réaction à ces préoccupations actuelles, l'UE a mis en place le Règlement général sur la protection des données (RGPD) le 4 avril 2016, au terme de nombreuses années de négociations et mesures législatives. La date d'entrée en vigueur du RGPD a été fixée au 25 mai 2018, posant un nouveau défi pour la protection des données personnelles.

Champ d'application du RGPD

On est généralement tenté de croire que si le RGPD a été mis au point par l'UE, il ne concerne pas les entreprises situées hors de ses frontières – ce qui n'est pourtant absolument pas le cas. Le champ d'application du RGPD englobe non seulement les entreprises actives au sein de l'UE

mais aussi celles qui se trouvent hors UE et fournissent des services commerciaux et internet à des clients établis en Europe. Autrement dit, la situation géographique d'une entreprise importe peu. À partir du moment où elle traite les données personnelles de clients de l'Union européenne pour leur fournir des produits ou services, elle est tenue de se conformer au RGPD.

Exigences de conformité du RGPD pour les entreprises

Comment est-ce que le RGPD régit la protection des données personnelles au niveau des entreprises fournissant des services commerciaux et internet ?
1. Pour ce qui est du traitement des données, les entreprises sont tenues de se conformer aux principes suivants :
a) Légalité : l'utilisation, le traitement comme les transactions de données personnelles à des fins commerciales doivent répondre aux exigences légales du RGPD.
b) Équité : lors de l'exploitation et du traitement des données, les intérêts des sujets concernés doivent être dûment considérés. Sacrifier les intérêts des sujets de données au profit de bénéfices économiques ou d'un usage commercial de leurs données personnelles est strictement interdit.
c) Transparence : l'utilisation et l'échange de données sont uniquement permis lorsque le sujet de données a connaissance des médias, du cadre comme des fins de ces opérations. Il est strictement interdit de traiter ou de négocier des données sans en faire part, au préalable, au sujet concerné.

De plus, les principes d' « impératifs catégoriques », de « minimisation des données », d' « exactitude », de « limitation du stockage », d' « intégrité et confidentialité » et de « reddition des comptes » sont également énoncés dans le RGPD.
2. Les entreprises doivent mettre en place une politique interne de reddition des comptes.
Elles doivent arrêter des dispositions institutionnelles exhaustives, incluant notamment des procédures de gestion de la sécurité des données, des méthodes de d'identification de fuites de données, des politiques de notification de violation des données pour répondre aux exigences rigoureuses de la « Directive ».
a) Délégué à la Protection des Données (DPO) : les entreprises doivent

désigner un délégué à la protection des données, chargé de communiquer avec l'autorité de contrôle de la protection des données. Le délégué à la protection des données doit présenter des rapports au comité du RGPD et est habilité à superviser le traitement des données auquel procède l'entreprise.

b) Documentation de la gestion des données : les entreprises sont tenues de recenser toutes les opérations de traitement des données en créant des fichiers consultables pour chacune d'elles. La gestion documentée est, outre une procédure de gestion interne, l'instrument de l'autorité de protection des données pour garantir que ces mesures soient respectées.

c) Analyse d'impact relative à la protection des données et consultation préalable : les entreprises doivent d'abord effectuer une analyse d'impact relative à la protection des données pour ce qui est des opérations de traitement de données très sensibles. Si l'analyse révèle qu'elles sont exposées à un haut risque et que l'entreprise concernée n'a aucun dispositif en place pour réduire le risque encouru, celle-ci doit se concerter préalablement avec l'autorité de protection des données quant aux opérations de traitement des données.

d) Intervention opérationnelle : les entreprises doivent disposer d'un plan d'intervention en cas de violation des données collectées. Dans ces circonstances, l'entreprise doit en référer à l'autorité de contrôle des données dans un délai de 72 heures.

e) Mesures de garantie de la sécurité : les entreprises doivent prendre les mesures suivantes pour assurer la sécurité des données :
1. Anonymisation et pseudonymisation des données personnelles.
2. Garantir à long terme la confidentialité, l'intégrité et l'exploitabilité des données comme des moyens de récupération systématique.
3. Récupération immédiate et accessibilité des données en cas d'erreurs de manipulation ou de défaillances techniques.
4. Définir des mesures de gestion, d'évaluation technique, d'analyse et de tests périodiques pour s'assurer de la validité du dispositif en place.

Droits individuels dans le cadre du RGPD

Le RGPD prévoit un ensemble de droits plus complets quant aux modes de traitement des données personnelles, de sorte à nous assurer un contrôle et une meilleure protection de nos données.

Quels types de droits nous accorde le RGPD ?
Le RGPD garantit aux propriétaires de données personnelles des droits substantiels par une réglementation détaillée portant sur les droits de savoir, d'accès, d'opposition, d'effacement et à la portabilité des données que détient le sujet de données.

I Droit de savoir : le contrôleur des données doit informer les citoyens de manière claire et concise quant aux modes de collecte et de traitement de leurs données.

I Droit d'accès : le contrôleur de données doit mettre à disposition des citoyens un moyen d'accès à leurs données. S'ils en font la demande par voie électronique, ces données doivent également leur être communiquées par voie électronique.

I Droit d'opposition : les sujets de données sont en droit de s'opposer, à tout moment, au traitement de leurs données personnelles par le contrôleur de données comme de refuser que celles-ci soient exploitées à des fins de marketing. La « Directive » prévoit également un droit à la limitation de leur traitement ; lorsque le sujet de données dépose une plainte (concernant, par exemple, l'exactitude de ses données), il peut imposer au contrôleur de données de limiter leur traitement, au lieu d'exiger leur effacement.

I Droit à la portabilité des données : les citoyens peuvent aisément transférer leurs documents et données personnelles d'un fournisseur de services d'information à un autre. Autrement dit, le sujet de données possède des droits substantiels quant au contrôle et au traitement de ses données personnelles.

I Droit à l'effacement des données : les sujets de données sont autorisés à demander au contrôleur de données que celles les concernant soient effacées et non diffusées. La finalité de ce droit est de remédier aux risques d'atteinte à la confidentialité liés au stockage de volumes importants de données personnelles, pour renforcer in fine la protection de la vie privée du sujet de données.

Sanctions sévères prévues par le RGPD

En plus de définir une série de lois uniformisées et de réglementations plus strictes pour le traitement des données personnelles, le RGPD prévoit également de lourdes peines en cas de violations et ce, sous forme d'amendes administratives. Ces sanctions s'appliquent à toute structure

dont les activités enfreignent le RGPD. Il existe deux niveaux de sanctions, suivant le degré d'infraction :

1. 10 millions d'euros ou 2% du chiffre d'affaires mondial annuel
2. 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel

L'objectif de ces sanctions sévères est d'obliger les entreprises à veiller à rester conformes au RGPD. Pour ne pas les encourir, il est essentiel d'éviter les fuites de données personnelles et de mettre en place des procédures de contrôle appropriées pour leur traitement.

Dahua et le respect du RGPD

Dahua Technology, l'un des principaux fournisseurs de solutions dans l'industrie mondiale de la vidéosurveillance, met depuis toujours un point d'honneur à la protection de la vie privée et la sécurité des données.

Depuis l'introduction du RGPD, Dahua accorde d'autant plus d'importance à la protection des données personnelles – chaque enregistrement vidéo comportant, en effet, un certain nombre de données personnelles. La conception des produits Dahua respecte les principes de légalité, d'équité et de transparence dictés par le RGPD quant au traitement de ces données. Prévoyant un ensemble de mesures pour leur protection, les produits Dahua cryptent les données personnelles afin d'assurer leur anonymisation et pseudonymisation. Au niveau des systèmes de gestion, Dahua continuera à optimiser sa procédure de protection des données en définissant des méthodes de gestion internes plus exhaustives ainsi qu'en améliorant sa reddition de comptes.

Utiliser les produits Dahua facilite votre mise en conformité avec le RGPD. À l'avenir, nous allons développer davantage de fonctionnalités permettant d'implémenter des solutions de sécurité supérieures, pour une meilleure protection de la vie privée.